

10-30-00

Practitioner's Docket No. 324-009927-US(PAR)

PATENT

JC921 U.S. PTO
09/698774
10/27/00

JC931 U.S. PTO
10/27/00

Preliminary Classification:

Proposed Class:

Subclass:

NOTE: "All applicants are requested to include a preliminary classification on newly filed patent applications. The preliminary classification, preferably class and subclass designations, should be identified in the upper right-hand corner of the letter of transmittal accompanying the application papers, for example 'Proposed Class 2, subclass 129.'" M.P.E.P. § 601, 7th ed.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231

NEW APPLICATION TRANSMITTAL

Transmitted herewith for filing is the patent application of

Inventor(s): Nouri ALLAHWERDI, Lassi HIPPELAINEN

WARNING: 37 C.F.R. § 1.41(a)(1) points out:

"(a) A patent is applied for in the name or names of the actual inventor or inventors.

"(1) The inventorship of a nonprovisional application is that inventorship set forth in the oath or declaration as prescribed by § 1.63, except as provided for in § 1.53(d)(4) and § 1.63(d). If an oath or declaration as prescribed by § 1.63 is not filed during the pendency of a nonprovisional application, the inventorship is that inventorship set forth in the application papers filed pursuant to § 1.53(b), unless a petition under this paragraph accompanied by the fee set forth in § 1.17(f) is filed supplying or changing the name or names of the inventor or inventors."

For (title): METHOD AND ARRANGEMENT FOR RELIABLY IDENTIFYING A USER IN A COMPUTER SYSTEM

CERTIFICATION UNDER 37 C.F.R. § 1.10*

(Express Mail label number is mandatory.)

(Express Mail certification is optional.)

I hereby certify that this New Application Transmittal and the documents referred to as attached therein are being deposited with the United States Postal Service on this date October 27, 2000, in an envelope as "Express Mail Post Office to Addressee," mailing Label Number EL627420688US, addressed to the: Assistant Commissioner for Patents, Washington, D.C. 20231.

Debra G. Conrad

(type or print name of person mailing paper)

Debra G. Conrad

Signature of person mailing paper

WARNING: Certificate of mailing (first class) or facsimile transmission procedures of 37 C.F.R. § 1.8 cannot be used to obtain a date of mailing or transmission for this correspondence.

*WARNING: Each paper or fee filed by "Express Mail" must have the number of the "Express Mail" mailing label placed thereon prior to mailing. 37 C.F.R. § 1.10(b).

"Since the filing of correspondence under § 1.10 without the Express Mail mailing label thereon is an oversight that can be avoided by the exercise of reasonable care, requests for waiver of this requirement will not be granted on petition." Notice of Oct. 24, 1996, 60 Fed. Reg. 56,439, at 56,442.

(New Application Transmittal [4-1]—page 1 of 11)

09698774-102700

1. Type of Application

This new application is for a(n)

(check one applicable item below)

- ☒ Original (nonprovisional)
☐ Design
☐ Plant

WARNING: Do not use this transmittal for a completion in the U.S. of an International Application under 35 U.S.C. § 371(c)(4), unless the International Application is being filed as a divisional, continuation or continuation-in-part application.

WARNING: Do not use this transmittal for the filing of a provisional application.

NOTE: If one of the following 3 items apply, then complete and attach **ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF A PRIOR U.S. APPLICATION CLAIMED** and a **NOTIFICATION IN PARENT APPLICATION OF THE FILING OF THIS CONTINUATION APPLICATION**.

- ☐ Divisional.
☐ Continuation.
☐ Continuation-in-part (C-I-P).

2. Benefit of Prior U.S. Application(s) (35 U.S.C. §§ 119(a), 120, or 121)

NOTE: A nonprovisional application may claim an invention disclosed in one or more prior filed copending nonprovisional applications or copending international applications designating the United States of America. In order for a nonprovisional application to claim the benefit of a prior filed copending nonprovisional application or copending international application designating the United States of America, each prior application must name as an inventor at least one inventor named in the later filed nonprovisional application and disclose the named inventor's invention claimed in at least one claim of the later filed nonprovisional application in the manner provided by the first paragraph of 35 U.S.C. § 112. Each prior application must also be:

(i) An international application entitled to a filing date in accordance with PCT Article 11 and designating the United States of America; or

(ii) Complete as set forth in § 1.51(b); or

(iii) Entitled to a filing date as set forth in § 1.53(b) or § 1.53(d) and include the basic filing fee set forth in § 1.16; or

(iv) Entitled to a filing date as set forth in § 1.53(b) and have paid therein the processing and retention fee set forth in § 1.21(f) within the time period set forth in § 1.53(f).

37 C.F.R. § 1.78(e)(1).

NOTE: If the new application being transmitted is a divisional, continuation or a continuation-in-part of a parent case, or where the parent case is an International Application which designated the U.S., or benefit of a prior provisional application is claimed, then check the following item and complete and attach **ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED**.

WARNING: If an application claims the benefit of the filing date of an earlier filed application under 35 U.S.C. §§ 120, 121 or 365(c), the 20-year term of that application will be based upon the filing date of the earliest U.S. application that the application makes reference to under 35 U.S.C. §§ 120, 121 or 365(c). (35 U.S.C. § 154(e)(2) does not take into account, for the determination of the patent term, any application on which priority is claimed under 35 U.S.C. §§ 119, 365(a) or 365(b).) For a c-p application, applicant should review whether any claim in the patent that will issue is supported by an earlier application and, if not, the applicant should consider canceling the reference to the earlier filed application. The term of a patent is not based on a claim-by-claim approach. See Notice of April 14, 1995, 60 Fed. Reg. 20,195, at 20,205.

(New Application Transmittal [4-1]—page 2 of 11)

002201-4286960

WARNING: When the last day of pendency of a provisional application falls on a Saturday, Sunday, or Federal holiday within the District of Columbia, any nonprovisional application claiming benefit of the provisional application must be filed prior to the Saturday, Sunday, or Federal holiday within the District of Columbia. See 37 C.F.R. § 1.78(a)(3).

- ☐ The new application being transmitted claims the benefit of prior U.S. application(s). Enclosed are ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED.

3. Papers Enclosed

A. Required for filing date under 37 C.F.R. § 1.53(b) (Regular) or 37 C.F.R. § 1.153 (Design) Application

14 Pages of specification

4 Pages of claims

4 Sheets of drawing

WARNING: DO NOT submit original drawings. A high quality copy of the drawings should be supplied when filing a patent application. The drawings that are submitted to the Office must be on strong, white, smooth, and non-shiny paper and meet the standards according to § 1.84. If corrections to the drawings are necessary, they should be made to the original drawing and a high-quality copy of the corrected original drawing then submitted to the Office. Only one copy is required or desired. For comments on proposed then-new 37 C.F.R. § 1.84, see Notice of March 9, 1988 (1990 O.G. 57-62).

NOTE: "Identifying indicia, if provided, should include the application number or the title of the invention, inventor's name, docket number (if any), and the name and telephone number of a person to call if the Office is unable to match the drawings to the proper application. This information should be placed on the back of each sheet of drawing a minimum distance of 1.5 cm. (5/8 inch) down from the top of the page . . ." 37 C.F.R. § 1.84(c)).

(complete the following, if applicable)

- ☐ The enclosed drawing(s) are photograph(s), and there is also attached a "PETITION TO ACCEPT PHOTOGRAPH(S) AS DRAWING(S)." 37 C.F.R. § 1.84(b).

☐ formal

☐ informal

B. Other Papers Enclosed

 Pages of declaration and power of attorney

1 Pages of abstract

 Other

4. Additional papers enclosed

☐ Amendment to claims

- ☐ Cancel in this applications claims _____ before calculating the filing fee. (At least one original independent claim must be retained for filing purposes.)

☐ Add the claims shown on the attached amendment. (Claims added have been numbered consecutively following the highest numbered original claims.)

☒ Preliminary Amendment

☐ Information Disclosure Statement (37 C.F.R. § 1.98)

☐ Form PTO-1449 (PTO/SB/08A and 08B)

☐ Citations

(New Application Transmittal [4-1]—page 3 of 11)

002201-4266960

- ☐ Declaration of Biological Deposit
- ☐ Submission of "Sequence Listing," computer readable copy and/or amendment pertaining thereto for biotechnology invention containing nucleotide and/or amino acid sequence.
- ☐ Authorization of Attorney(s) to Accept and Follow Instructions from Representative
- ☐ Special Comments
- ☐ Other

5. Declaration or oath (Including power of attorney)

NOTE: A newly executed declaration is not required in a continuation or divisional application provided that the prior nonprovisional application contained a declaration as required, the application being filed is by all or fewer than all the inventors named in the prior application, there is no new matter in the application being filed, and a copy of the executed declaration filed in the prior application (showing the signature or an indication thereon that it was signed) is submitted. The copy must be accompanied by a statement requesting deletion of the names of person(s) who are not inventors of the application being filed. If the declaration in the prior application was filed under § 1.47, then a copy of that declaration must be filed accompanied by a copy of the decision granting § 1.47 status or, if a nonsigning person under § 1.47 has subsequently joined in a prior application, then a copy of the subsequently executed declaration must be filed. See 37 C.F.R. §§ 1.63(d)(1)-(3).

NOTE: A declaration filed to complete an application must be executed, identify the specification to which it is directed, identify each inventor by full name including family name and at least one given name, without abbreviation together with any other given name or initial, and the residence, post office address and country or citizenship of each inventor, and state whether the inventor is a sole or joint inventor. 37 C.F.R. § 1.63(a)(1)-(4).

- ☐ Enclosed
- Executed by

(check all applicable boxes)

- ☐ inventor(s).
- ☐ legal representative of inventor(s).
37 C.F.R. §§ 1.42 or 1.43.
- ☐ joint inventor or person showing a proprietary interest on behalf of inventor who refused to sign or cannot be reached.
 - ☐ This is the petition required by 37 C.F.R. § 1.47 and the statement required by 37 C.F.R. § 1.47 is also attached. See item 13 below for fee.

☒ Not Enclosed.

NOTE: Where the filing is a completion in the U.S. of an International Application or where the completion of the U.S. application contains subject matter in addition to the International Application, the application may be treated as a continuation or continuation-in-part, as the case may be, utilizing ADDED PAGE FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION CLAIMED.

- ☒ Application is made by a person authorized under 37 C.F.R. § 1.41(c) on behalf of all the above named inventor(s).

(The declaration or oath, along with the surcharge required by 37 C.F.R. § 1.16(e) can be filed subsequently).

- ☐ Showing that the filing is authorized.
(not required unless called into question. 37 C.F.R. § 1.41(d))

6. Inventorship Statement

WARNING: If the named inventors are each not the inventors of all the claims an explanation, including the ownership of the various claims at the time the last claimed invention was made, should be submitted.

The inventorship for all the claims in this application are:

☐ The same.

or

☐ Not the same. An explanation, including the ownership of the various claims at the time the last claimed invention was made,

☐ is submitted.

☐ will be submitted.

7. Language

NOTE: An application including a signed oath or declaration may be filed in a language other than English. An English translation of the non-English language application and the processing fee of \$130.00 required by 37 C.F.R. § 1.17(h) is required to be filed with the application, or within such time as may be set by the Office. 37 C.F.R. § 1.52(d).

☒ English

☐ Non-English

☐ The attached translation includes a statement that the translation is accurate. 37 C.F.R. § 1.52(d).

8. Assignment

☒ An assignment of the invention to Nokia Mobile Phones Ltd.

☐ is attached. A separate ☐ "COVER SHEET FOR ASSIGNMENT (DOCUMENT) ACCOMPANYING NEW PATENT APPLICATION" or ☐ FORM PTO 1595 is also attached.

☒ will follow.

NOTE: "If an assignment is submitted with a new application, send two separate letters—one for the application and one for the assignment." Notice of May 4, 1990 (1114 O.G. 77-78).

WARNING: A newly executed "CERTIFICATE UNDER 37 C.F.R. § 3.73(b)" must be filed when a continuation-in-part application is filed by an assignee. Notice of April 30, 1993, 1150 O.G. 62-64.

(New Application Transmittal [4-1]—page 5 of 11)

002201"4265960

9. Certified Copy

Certified copy(ies) of application(s)

Country	Appln. No.	Filed
Finland	19992343	29 October 1999
Country	Appln. No.	Filed
Country	Appln. No.	Filed

from which priority is claimed

☒ is (are) attached.☐ will follow.

NOTE: The foreign application forming the basis for the claim for priority must be referred to in the oath or declaration. 37 C.F.R. § 1.55(a) and 1.63.

NOTE: This item is for any foreign priority for which the application being filed directly relates. If any parent U.S. application or International Application from which this application claims benefit under 35 U.S.C. § 120 is itself entitled to priority from a prior foreign application, then complete Item 18 on the ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED.

10. Fee Calculation (37 C.F.R. § 1.16)**A.** ☒ Regular application

CLAIMS AS FILED					Basic Fee	
Number filed	Number Extra		Rate		37 C.F.R. § 1.16(a)	
					\$ 710.00	
Total Claims (37 C.F.R. § 1.16(c))	19	- 20 =	0	×	\$ 18.00	0
Independent Claims (37 C.F.R. § 1.16(b))	2	- 3 =	0	×	\$ 80.00	0
Multiple dependent claim(s), If any (37 C.F.R. § 1.16(d))				+	\$ 270.00	

☐ Amendment cancelling extra claims is enclosed.☒ Amendment deleting multiple-dependencies is enclosed.☐ Fee for extra claims is not being paid at this time.

NOTE: If the fees for extra claims are not paid on filing they must be paid or the claims cancelled by amendment, prior to the expiration of the time period set for response by the Patent and Trademark Office in any notice of fee deficiency. 37 C.F.R. § 1.16(d).

Filing Fee Calculation

\$ 710.00

B. ☐ Design application

(\$ 320.00 - 37 C.F.R. § 1.16(f))

Filing Fee Calculation

\$ _____

C. ☐ Plant application

(\$ 490.00 - 37 C.F.R. § 1.16(g))

Filing fee calculation

\$ _____

11. Small Entity Statement(s)

- ☐ Statement(s) that this is a filing by a small entity under 37 C.F.R. § 1.9 and 1.27 is (are) attached.

WARNING: "Status as a small entity must be specifically established in each application or patent in which the status is available and desired. Status as a small entity in one application or patent does not affect any other application or patent, including applications or patents which are directly or indirectly dependent upon the application or patent in which the status has been established. The refiling of an application under § 1.53 as a continuation, division, or continuation-in-part (including a continued prosecution application under § 1.53(d)), or the filing of a reissue application requires a new determination as to continued entitlement to small entity status for the continuing or reissue application. A nonprovisional application claiming benefit under 35 U.S.C. § 119(e), 120, 121, or 365(c) of a prior application, or a reissue application may rely on a statement filed in the prior application or in the patent if the nonprovisional application or the reissue application includes a reference to the statement in the prior application or in the patent or includes a copy of the statement in the prior application or in the patent and status as a small entity is still proper and desired. The payment of the small entity basic statutory filing fee will be treated as such a reference for purposes of this section." 37 C.F.R. § 1.28(a)(2).

WARNING: "Small entity status must not be established when the person or persons signing the . . . statement can unequivocally make the required self-certification." M.P.E.P., § 509.03, 6th ed., rev. 2, July 1996 (emphasis added).

(complete the following, if applicable)

- ☐ Status as a small entity was claimed in prior application _____ / _____, filed on _____, from which benefit is being claimed for this application under:

35 U.S.C. § ☐ 119(e),
☐ 120,
☐ 121,
☐ 365(c),

and which status as a small entity is still proper and desired.

- ☐ A copy of the statement in the prior application is included.

Filing Fee Calculation (50% of A, B or C above)

\$ _____

NOTE: Any excess of the full fee paid will be refunded if small entity status is established and a refund request are filed within 2 months of the date of timely payment of a full fee. The two-month period is not extendable under § 1.136. 37 C.F.R. § 1.28(a).

12. Request for International-Type Search (37 C.F.R. § 1.104(d))

(complete, if applicable)

- ☐ Please prepare an international-type search report for this application at the time when national examination on the merits takes place.

13. Fee Payment Being Made at This Time

☐ Not Enclosed

☐ No filing fee is to be paid at this time.

(This and the surcharge required by 37 C.F.R. § 1.16(e) can be paid subsequently.)

☒ Enclosed

☒ Filing fee

\$ 710.00

☐ Recording assignment

(\$40.00; 37 C.F.R. § 1.21(h))

(See attached "COVER SHEET FOR
ASSIGNMENT ACCOMPANYING NEW
APPLICATION".)

\$ _____

☐ Petition fee for filing by other than all the
inventors or person on behalf of the inventor
where inventor refused to sign or cannot be
reached

(\$130.00; 37 C.F.R. §§ 1.47 and 1.17(l))

\$ _____

☐ For processing an application with a
specification in

a non-English language

(\$130.00; 37 C.F.R. §§ 1.52(d) and 1.17(k))

\$ _____

☐ Processing and retention fee

(\$130.00; 37 C.F.R. §§ 1.53(d) and 1.21(l))

\$ _____

☐ Fee for international-type search report

(\$40.00; 37 C.F.R. § 1.21(e))

\$ _____

NOTE: 37 C.F.R. § 1.21(l) establishes a fee for processing and retaining any application that is abandoned for failing to complete the application pursuant to 37 C.F.R. § 1.53(f) and this, as well as the changes to 37 C.F.R. §§ 1.53 and 1.78(a)(1), indicate that in order to obtain the benefit of a prior U.S. application, either the basic filing fee must be paid, or the processing and retention fee of § 1.21(l) must be paid, within 1 year from notification under § 53(f).

Total fees enclosed

\$ 710.00

14. Method of Payment of Fees

☒ Check in the amount of \$ 710.00

☐ Charge Account No. _____ in the amount of
\$ _____

A duplicate of this transmittal is attached.

NOTE: Fees should be itemized in such a manner that it is clear for which purpose the fees are paid. 37 C.F.R. § 1.22(b).

15. Authorization to Charge Additional Fees

WARNING: If no fees are to be paid on filing, the following items should not be completed.

WARNING: Accurately count claims, especially multiple dependent claims, to avoid unexpected high charges, if extra claim charges are authorized.

- ☒ The Commissioner is hereby authorized to charge the following additional fees by this paper and during the entire pendency of this application to Account No. 16-1350:

☒ 37 C.F.R. § 1.16(a), (f) or (g) (filing fees)

☒ 37 C.F.R. § 1.16(b), (c) and (d) (presentation of extra claims)

NOTE: Because additional fees for excess or multiple dependent claims not paid on filing or on later presentation must only be paid or these claims cancelled by amendment prior to the expiration of the time period set for response by the PTO in any notice of fee deficiency (37 C.F.R. § 1.16(d)), it might be best not to authorize the PTO to charge additional claim fees, except possibly when dealing with amendments after final action.

☒ 37 C.F.R. § 1.16(e) (surcharge for filing the basic filing fee and/or declaration on a date later than the filing date of the application)

☒ 37 C.F.R. § 1.17(a)(1)-(5) (extension fees pursuant to § 1.136(a)).

☒ 37 C.F.R. § 1.17 (application processing fees)

NOTE: ". . . A written request may be submitted in an application that is an authorization to treat any concurrent or future reply, requiring a petition for an extension of time under this paragraph for its timely submission, as incorporating a petition for extension of time for the appropriate length of time. An authorization to charge all required fees, fees under § 1.17, or all required extension of time fees will be treated as a constructive petition for an extension of time in any concurrent or future reply requiring a petition for an extension of time under this paragraph for its timely submission. Submission of the fee set forth in § 1.17(a) will also be treated as a constructive petition for an extension of time in any concurrent reply requiring a petition for an extension of time under this paragraph for its timely submission." 37 C.F.R. § 1.136(a)(3).

☐ 37 C.F.R. § 1.18 (issue fee at or before mailing of Notice of Allowance, pursuant to 37 C.F.R. § 1.311(b))

NOTE: Where an authorization to charge the issue fee to a deposit account has been filed before the mailing of a Notice of Allowance, the issue fee will be automatically charged to the deposit account at the time of mailing the notice of allowance. 37 C.F.R. § 1.311(b).

NOTE: 37 C.F.R. § 1.28(b) requires "Notification of any change in status resulting in loss of entitlement to small entity status must be filed in the application . . . prior to paying, or at the time of paying, . . . the issue fee. . . ." From the wording of 37 C.F.R. § 1.28(b), (a) notification of change of status must be made even if the fee is paid as "other than a small entity" and (b) no notification is required if the change is to another small entity.

16. Instructions as to Overpayment

NOTE: "... Amounts of twenty-five dollars or less will not be returned unless specifically requested within a reasonable time, nor will the payer be notified of such amounts; amounts over twenty-five dollars may be returned by check or, if requested, by credit to a deposit account." 37 C.F.R. § 1.26(a).

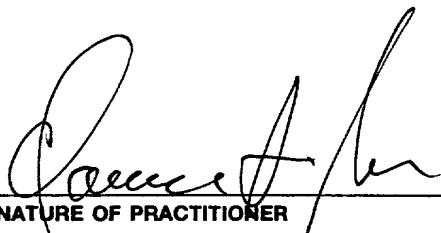
- ☒ Credit Account No. 16-1350
☐ Refund

SEND ALL CORRESPONDENCE TO:
Clarence A. Green, Reg. No.: 24,622
PERMAN & GREEN, LLP
425 Post Road
Fairfield, Connecticut 06430

Reg. No. 24,622

Tel. No. (203) 259-1800

Customer No. 2512



SIGNATURE OF PRACTITIONER
Clarence A. Green
(type or print name of attorney)
PERMAN & GREEN, LLP

P.O. Address
425 Post Road, Fairfield, Connecticut 06430

002207 426550

☐ **Incorporation by reference of added pages**

(check the following item if the application in this transmittal claims the benefit of prior U.S. application(s) (including an international application entering the U.S. stage as a continuation, divisional or C-I-P application) and complete and attach the ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED)

- ☐ Plus Added Pages for New Application Transmittal Where Benefit of Prior U.S. Application(s) Claimed

Number of pages added _____

- ☐ Plus Added Pages for Papers Referred to in Item 4 Above

Number of pages added _____

- ☐ Plus added pages deleting names of inventor(s) named in prior application(s) who is/are no longer inventor(s) of the subject matter claimed in this application.

Number of pages added _____

- ☐ Plus "Assignment Cover Letter Accompanying New Application"

Number of pages added _____

☒ **Statement Where No Further Pages Added**

(if no further pages form a part of this Transmittal, then end this Transmittal with this page and check the following item)

- ☒ This transmittal ends with this page.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Express Mail No.: EL627420688US

In re Application of: ALLAHWERDI et al.

SERIAL NUMBER:

EXAMINER:

FILING DATE: Herewith

ART UNIT:

TITLE: METHOD AND ARRANGEMENT FOR RELIABLY IDENTIFYING A
USER IN A COMPUTER SYSTEM

ATTORNEY DOCKET NO.: 324-009927-US(PAR)

The Commissioner of Patents and Trademarks

Washington, D.C. 20231

PRELIMINARY AMENDMENT

Dear Sir:

Please amend the above-identified, enclosed patent application as follows:

IN THE CLAIMS:

Please amend Claims 8, 9, 17, 18 and 19 as shown below.

Claim 8, line 1, delete “any one of preceding claims 1 to 7” and insert --claim 1--.

Claim 9, line 1, delete “or 7”.

Claim 17, line 1, delete “claims 15 or 16” and insert --claim 15--.

Claim 18, lines 1 and 2, delete “any one of preceding claims 10 to 17” and insert --
claim 10--.

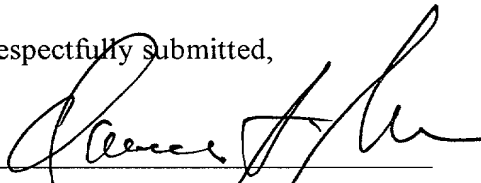
002207 4286960

Claim 19, lines 1 and 2, delete "any one of preceding claims 10 to 17" and insert -- claim 10--.

REMARKS

Please enter this preliminary amendment prior to calculation of the fees.

Respectfully submitted,



Clarence A. Green, Reg. No. 24,622

Perman & Green, LLP

425 Post Road

Fairfield, CT 06430

(203) 259-1800 Customer No. 2512



Date

0069874-102700

METHOD AND ARRANGEMENT FOR RELIABLY IDENTIFYING A USER IN A COMPUTER SYSTEM

FIELD OF THE INVENTION

The invention relates to a method and arrangement for reliably
 5 identifying a user in a computer system. The invention particularly relates to a solution wherein a connection to a computer system is implemented by a mobile station, preferably a mobile station in a mobile telephone system.

BACKGROUND OF THE INVENTION

Most computer systems have been designed such that users have
 10 to log into a system from their own workstation by using their unique user name and password. A server of the system, typically an authentication server, checks whether such a user name has been defined among the users of the system and whether a given password corresponds with said user name. If so, the user is allowed to access the system; otherwise no access is
 15 allowed. This is to guarantee that the system is secure, i.e. to prevent unauthorized users from accessing the system. When the workstations have a fixed connection to the computer system through, for example, integrated cabling, this method of identifying users usually suffices.

Nowadays, however, remote connections are often needed in a
 20 computer system. This means that the user's workstation does not have a fixed connection to the computer system but the connection is established through a public network, typically a telephone network. Through a modem, for example, the workstation is connected to the telephone network, through which a telephone connection is established to the system through a modem
 25 series of the system. In such a case, much more is required of the identification of the user because the connection is established through a public telephone network whose security cannot be controlled by the system administrator. Identifying users on the basis of user names and passwords in a connection established over a public network is dubious since unauthorized access to the system then becomes possible by e.g. guessing the user names
 30 and passwords. User names are often formed from the names of the users, and if the users themselves may choose their passwords, they are quite often easy to infer or guess.

The connections between a terminal and a computer system are
 35 often implemented by using a protocol called a PPP (Point-to-Point) protocol.

PPP connections often utilize methods called a CHAP (Challenge-Handshake Authentication Protocol) method or a PAP (Password Authentication Protocol) method. In the PAP method, a password is transferred over a transmission path unencrypted, so the protection it provides is quite weak. The CHAP method utilizes an encrypted password. In the method, the same algorithm is applied at both ends of the transmission path. The network transmits a random number to the terminal, which computes a secret value on the basis of the number, user name and password by utilizing the algorithm. The secret value, password and user name are transmitted to the network, which computes a password from the secret value and compares it with the transmitted password.

It is further known to use a method called a RADIUS (Remote Authentication Dial In User Service Protocol, RFC 2138) method when a user logs in.

Various methods have also been developed for enhancing the reliability and security in identifying a user of a computer system. Since passwords defined by the user are often easy to crack, the prior art solutions utilize one-time passwords. Hence, each password is only used once when the user logs in, and even if a third party were to crack the password, it would be of no use since another password would be used the next time. In this method, both the user and the authentication server of the computer system must have corresponding password lists available. The user may have the password list written on paper, for example, or alternatively, a separate device called a trusted device may be used to generate one-time passwords.

US 5 485 519 discloses a method wherein a user has a separate device to generate a password. The user enters a predetermined password into the device, which forms from the password and encrypted bit sequence programmed into the device a password to be used on the connection. This password is encrypted and stored in the device to be used for generating the next password. In the solution of the publication, the password generated by the device has to be inputted into a processor apparatus establishing the connection, such as a computer, for example, through a magnetic tape reader or diskette drive.

US 4 720 860 discloses a solution utilizing one-time passwords wherein a user has a separate device, e.g. a card of the smart card type, which generates a one-time password to be read by the user from the display

of the device and entered by the user into a computer operating as a means of communication. The device generates a one-time code on the basis of a fixed code and a varying parameter, such as time. The fixed code is programmed in the device. It is also feasible that the fixed code is inputted into the device. The authentication server of the computer system calculates a second identification number by utilizing the same parameters, and if the identification numbers match, the connection is allowed and feasible.

US 5 657 388, US 5 373 559 and US 5 491 752 disclose another solution utilizing one-time passwords wherein a user has a simple, separate device called a token, such as a memory card, for example, with a secret code stored therein. A means of communication, a portable computer, for example, reads the secret code from the memory of the card. The user enters his or her personal password into the communication means, which generates a one-time password on the basis of the secret code, password and time, and which then transmits the generated password to the authentication server of the computer system.

In all prior art solutions described above, the user has to carry with him several devices, i.e. a separate password generator, typically a card of the smart card type, and the actual communication means for establishing a connection to the desired computer system. Furthermore, in all known solutions, the user has to actively either enter the one-time password read from the smart card into the communication means or alternatively, supply the entire card into the communication means, thus enabling the data in the card to be read.

BRIEF DESCRIPTION OF THE INVENTION

An object of the invention is thus to provide a method and an arrangement implementing the method such that a user can be identified in a reliable manner without, however, causing any trouble or inconvenience to the user. This is achieved by a method of reliably identifying a user in a computer system, in which method a mobile station is used for communicating with the computer system and a personal identification number is supplied into the mobile station.

The method of the invention comprises generating a first one-time password in the mobile station without any action by the user by utilizing a known algorithm on the basis of a personal identification number of the user,

subscriber-specific identifier read from a subscriber-specific identification module of the mobile station, device-specific identifier of the mobile station and time, encoding the first one-time password and the subscriber-specific identifier of the user at the mobile station, transmitting the encoded password and subscriber-specific identifier to an authentication server of the computer system, identifying the user at the authentication server on the basis of the subscriber-specific identifier, and searching a database for the personal identifier number of the user and the device-specific identifier of the mobile station associated with the user, generating a second one-time password at the authentication server by utilizing the predetermined algorithm on the basis of the personal identification number of the user, subscriber-specific identifier, device-specific identifier of the mobile station and time, comparing the first password and the second password with each other at the authentication server, and if the passwords match, enabling the telecommunication connection between the mobile station of the user and the computer system.

The invention further relates to an arrangement for reliably identifying a user in a computer system, which arrangement comprises a mobile station used for communicating with the computer system, the mobile station comprising a subscriber-specific identification module comprising a subscriber-specific identifier, a device-specific identifier permanently encoded in the mobile station, means for reading a personal identifier number which is supplied by the user and which enables the device to be used, means for checking the correctness of the identifier number always before the device is put to use, and which arrangement comprises an authentication server comprising memory means for storing the user names of the users in the system and the corresponding personal identifiers and device-specific identifiers.

In the arrangement of the invention, the mobile station comprises means for generating a first one-time password without any action by the user by utilizing a known algorithm on the basis of the personal identification number of the user, subscriber-specific identifier read from a subscriber-specific identification module of the mobile station, device-specific identifier of the mobile station and time, means for encoding the first one-time password and the subscriber-specific identifier of the user, means for transmitting the encoded password and subscriber-specific identifier to an authentication server of the computer system, and the authentication server is arranged to identify the user on the basis of the subscriber-specific identifier, and search a database for the

personal identifier number of the user and the device-specific identifier of the mobile station associated with the user, generate a second one-time password by utilizing the predetermined algorithm on the basis of the personal identification number of the user, subscriber-specific identifier, device-specific identifier of the mobile station and time, compare the first password and the second password with each other, and if the passwords match, enable the telecommunication connection between the mobile station of the user and the computer system.

The idea underlying the invention is that the mobile station itself is a "trusted device", which means that the user does not need any separate devices to carry with him when the user desires to establish a secure connection to the computer system. The solution of the invention also enables connection setup to be automatized without the security being disturbed.

In the solution of the invention, the mobile station, which establishes a connection to the computer system, thus itself generates the necessary one-time password. The password is generated by utilizing a predetermined algorithm having time, subscriber identifier of the user, device identifier of the mobile station and the PIN code of the user as its parameters.

Several advantages are achieved by the method and arrangement of the invention. A drawback of the previous solutions, i.e. the use of two separate devices, can be avoided. Further, the connection setup process itself is quicker since at this stage the user does not have to enter passwords into the device; external peripherals are also unnecessary. The solution of the invention also provides strict data security since a potential intruder will not benefit from intercepting the algorithms or programs used. Copied programs do not function in a foreign device even if the password of the user, or PIN, had been cracked.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is now described in closer detail in connection with the preferred embodiments and with reference to the accompanying drawings, in which

Figure 1 shows an example of a system whereto a solution of the invention can be applied,

Figures 2a and 2b are flow diagrams illustrating a method of the invention, and

Figure 3 illustrates an example of the structure of a mobile station of the invention.

DETAILED DESCRIPTION OF THE INVENTION

Referring to Figure 1, examine an example of a system where to a solution of the invention can be applied. In the solution of the invention, a user is in the possession of a mobile station 100, which is used for communicating with a desired computer system 102. Figure 1 only shows an example of a radio system of the invention. The details of the structure of the radio system and the connection to the computer system per se may also be implemented differently as long as the characteristics of the invention are taken into account. The solution of the invention is thus not restricted to a GPRS system only although such a system has been used as the example in Figure 1.

A radio network typically comprises a fixed network infrastructure, i.e. a network part 104, and subscriber terminals 100, which may be fixedly located, vehicle-mounted or portable terminals to be carried around. The network part 104 comprises base stations 106. A plurality of base stations 106 are, in turn, controlled in a centralized manner by a radio network controller 108 communicating with them. A base station 106 comprises transceivers 110 and a multiplexer unit 112.

The base station 106 further comprises a control unit 114, which controls the operation of the transceivers 110 and the multiplexer 112. The multiplexer 112 arranges the traffic and control channels used by several transceivers 110 to a single transmission connection 116.

The transceivers 110 of the base station 106 are connected to an antenna unit 118, which is used for implementing a bi-directional radio connection 120 to a subscriber terminal 100. The structure of the frames to be transmitted in the bi-directional radio connection 120 is defined system-specifically, and the connection is called an air interface.

The radio network controller 108 comprises a group switching field 122 and a control unit 124. The group switching field 124 is used for connecting speech and data and for combining signaling circuits. The base station 106 and the radio network controller 108 form a radio network subsystem 126, which further comprises a transcoder 128. The transcoder 128 is usually located as close to a mobile services switching center 130 as possible since speech can then be transferred in a cellular radio network form between the

transcoder 128 and the radio network controller 108 by using as little transmission capacity as possible.

The transcoder 128 converts the different digital speech coding forms used between a public switched telephone network and a mobile telephone network into compatible ones, for instance from a fixed network form to another cellular radio network form, and vice versa. The control unit 124 performs call control, mobility management, collection of statistical data and signaling.

Figure 1 further shows the mobile services switching center 130 and a gateway mobile services switching center 132, which is responsible for the connections from the mobile telephone system to the outside world, in this case to a public switched telephone network 134. The mobile telephone system also comprises various databases that maintain various information in order to maintain the functionality of the system. Such a register is an HLR (Home Location Register) 150, which comprises information associated with the subscribers in the system. The HLR maintains, for example, information on the whereabouts of a subscriber at a given time. The system further comprises a logically MSC-specific VLR (Visitor Location Register) 152, which maintains information on users located within the area of a given MCS at a given time, and information on the location of the users in a more specific manner than the HLR. Furthermore, the system comprises an EIR (Equipment Identity Register) 154, which maintains information on the terminals in the system. Each terminal typically comprises a device-specific device identifier, e.g. an IMEI (International Mobile Equipment Identifier), attached to the terminal already when the device was being manufactured, on the basis of which each terminal can be identified individually. The EIR maintains information on the device identifiers.

As can be seen from Figure 1, the group switching field 122 can be used for establishing connections both to the PSTN (Public Switched Telephone Network) 134 through the mobile services switching center 130 and to a packet transmission network 136.

The connection between the packet transmission network 136 and the group switching field 122 is established by an SGSN (Serving GPRS Support Node) 138. The SGSN 138 is responsible for transferring packets between the base station system and a GGSN (Gateway GPRS Support Node) 140, and for keeping a record of the location of the subscriber terminal 100 in

its area. The SGSN 138 may also communicate with databases 150 to 154 of the mobile telephone system either through the MSC 130 or directly.

The GGSN 140 combines a public packet transmission network 142 and the packet transmission network 132. An Internet protocol or X.25 protocol can be used on the interface. By encapsulation, the GGSN 140 hides the internal structure of the packet transmission network 136 from the public packet transmission network 142, so for the public packet transmission network 142, the packet transmission network 136 resembles a sub-network, the public packet transmission network being able to address packets to the subscriber terminal 100 located therein and to receive packets therefrom.

The packet transmission network 136 is typically a network utilizing the Internet protocol of the radio network operator and carrying signaling and tunnelled user data. As regards the architecture and protocols below the Internet protocol layer, the structure of the network 136 may vary operator-specifically.

The public packet transmission network 142 may be the global Internet, for example, to which the computer system 102 is connected.

The computer system 102 typically comprises an authentication server 144, which is responsible for authenticating users trying to access the system and allowing authorized users to access the rest of the system 146. The authentication server 144 is not necessarily a separate apparatus but it can also be implemented by software as a part of a computer. The authentication server also comprises a memory 148, in which the user names of the users in the system and the corresponding personal identifiers and device-specific identifiers have been stored. The memory can be implemented as a fixed part of the normal server equipment or as separate database equipment. The rest of the system 146 typically comprises one or more computer hardware configurations, which provide e-mail or database services and corresponding company network solutions.

A connection can be established to another data network 156, preferably a local network, such as a company intranet, through a second GGSN 140b. In the solution of the invention, a connection to a desired network requiring authentication can thus be established in many ways.

The present invention thus particularly relates to reliably identifying a user while establishing a connection to a computer system. Although the

identification must be reliable, it is also desirable that the identification procedure can be implemented smoothly as far as the user is concerned.

Examine an example of the solution of the invention by means of flow diagrams 2a and 2b. In step 200, a user switches on a mobile station. Typically, the mobile station is at this stage set to request the user to enter a password, i.e. PIN (Personal Identification Number), which enables the mobile station to be used. In step 202, the user enters the password into the mobile station. The mobile station can then also be used as a common telephone, but when the user in step 204 starts an application requiring a predetermined computer system, such as an e-mail program, the mobile station then, in the solution of the invention, generates a one-time password in step 206. This step will be described later in closer detail.

If the mobile station is not to be used for communication that requires encryption, the user can enter another predetermined password, i.e. PIN, into the mobile station while switching on the device. In a preferred embodiment of the invention, the user thus has at least two different passwords, and some of these passwords enable applications requiring encryption to be used while some do not. Hence, the mobile station can be safely used and, if desired, also lent to a second party unequipped to use applications requiring encryption.

Next, the mobile station typically encodes the generated password and the user name of the user in an appropriate manner and transmits a message to the computer system in step 208. The computer system receives the message, and in step 210, itself generates a corresponding one-time password and compares the passwords, and if the passwords match, grants access to the information in the system, and the connection can continue in step 212. If the passwords do not match, the system does not, in the preferred embodiment of the invention, transmit any response to the mobile station. This enhances security since a potential intruder will not find out why the connection failed.

The password and the user name can be transmitted to the computer system appropriately encrypted, either by using encryption specific to the radio system or unique encryption enhancing security, which can be decrypted by the receiving end. These steps can be implemented in ways known to one skilled in the art.

The generation of passwords is illustrated in closer detail in diagram 2b. In step 220, the mobile station synchronizes its internal clock with the system clock. The synchronization can be carried out by utilizing the known synchronization methods. The synchronization is to make sure that the mobile station and the system use the same time parameter in generating the passwords. In step 222, an "A subscriber identifier" A_SCRBR is read from a subscriber-specific identification module of the mobile station, such as an SIM/USIM ([Universal] Subscriber Identity Module) card, or the like.

In step 224, the device identifier of the mobile station is read. In the solution of the invention, each mobile station has a device-specific device identifier, e.g. an IMEI (International Mobile Equipment Identifier), attached to the mobile station when the mobile station was being manufactured, on the basis of which each mobile station can be identified individually. In the GSM system, for example, the IMEI identifier comprises the following fields:

- 15 TAC type approval code,
- FAC final assembly code,
- SNR serial number, and
- SVN software version number.

In step 226, the personal identifier number, or PIN, supplied by the user is read from the memory.

Using the aforementioned values (personal identification number, or PIN, of the user, subscriber-specific identifier A_SCRBR, device-specific identifier IMEI of the mobile station and time), the mobile station computes a one-time password by applying a predetermined algorithm. The predetermined algorithm can be fixedly programmed in the mobile station, or alternatively, it can be changeable, for example downloadable from the computer system.

In addition to the aforementioned values, it is also feasible to use numbers stored in the memory of the mobile station as an algorithm parameter. For example, a set of prime numbers can be downloaded from the computer system in table form. The same table is also known to the authentication server.

The mobile station can also be lent to another user if the PIN of the mobile station is changed, because it is then impossible to establish a connection to the computer system. The terminal can then either completely prevent the identification procedure from starting or the terminal can allow the identification procedure; in such a case, connection setup always fails anyway be-

cause of an incorrect PIN. Similarly, connection setup can be prevented also by changing the SIM card.

The characteristics of the invention can be implemented both in the mobile station and the computer system preferably by software. Examine next
5 an example of the structure of a mobile station by means of Figure 3.

Figure 3 shows an example of the structure of a mobile station 100. The mobile station comprises an antenna 300, which is used for transmitting and receiving signals. Examine first the receiver section. A signal received by the antenna 300 is supplied through a duplex filter 302 to a radio frequency receiver 304. The duplex filter separates the transmitting and receiving frequencies from each other. The radio frequency receiver 304 comprises a filter to block frequencies outside the desired frequency band. Next, the signal is converted to intermediate frequency or directly to baseband, and the baseband signal is sampled and quantized at an analogue/digital converter 306. An equalizer 308 compensates for interference caused by multipath propagation, for example. From the equalized signal, a demodulator 310 takes a bit stream, which is transmitted to a demultiplexer 312. The demultiplexer 312 separates the bit stream from different time slots into separate logical channels. A channel codec 314 decodes the bit streams of the separate logical channels, i.e. decides whether a bit stream is signaling data, which is transmitted to a control unit 316, or whether the bit stream is speech, which is transmitted to a speech codec 318, or data, which is transmitted to a data unit 320, for example. The data unit can be, for example, a display of the mobile station or a data processing unit, peripheral or the like. From the speech codec 318, a speech signal is forwarded to a loudspeaker 322. The channel codec 314 also performs error correction. The control unit 316 performs internal control functions by controlling the different units.

In the transmitter section, the channel codec 314 receives the signal to be transmitted either from the data unit 320 or the speech codec 318. The speech codec receives the signal from a microphone 324. The data unit may be, for example, a keypad or a touch-sensitive display or a peripheral of the mobile station. A burst generator 326 adds a training sequence and a tail to the data supplied from the channel codec 314. A multiplexer 328 assigns a time slot to each burst. A modulator 330 modulates digital signals to a radio frequency carrier. This is an analogue operation, therefore a digital/analogue converter 332 is needed for performing it. A transmitter 334 comprises a filter

to restrict the bandwidth. In addition, the transmitter 334 controls the output power of a transmission. A synthesizer 336 arranges the necessary frequencies for the different units. The synthesizer 336 generates the necessary frequencies by using a voltage controlled oscillator, for example.

5 In a manner shown in Figure 3, the structure of the transceiver can be further divided into radio frequency parts 338 and a digital signal processor including software 340. The radio frequency parts 338 comprise the duplex filter 302, receiver 304, transmitter 334 and synthesizer 336. The digital signal processor including the software 340 comprises the equalizer 308, demodu-
10 lator 310, demultiplexer 312, channel codec 314, control unit 316, burst generator 326, multiplexer 328 and modulator 330. The analogue/digital converter 306 is needed for converting an analogue radio signal to a digital one and, correspondingly, the digital/analogue converter 332 for converting a digital signal to an analogue one.

15 The mobile station further comprises a subscriber-specific reader 342 of the identification module, typically a SIM/USIM card reader or the like. When the mobile station is being switched on, the control unit 316 of the mobile station checks whether a card is inserted in the reader, and reads the user identification data from the card. When the mobile station was being manu-
20 factured, a device-specific identifier IMEI, which is readable by the control unit 316, was also stored in the mobile station in a memory element 344. The device-specific identifier is fixedly stored in a memory circuit and cannot be easily changed.

Naturally, the device of the invention may comprise different user
25 interface parts, such as a display and a keypad, but these parts are not described in closer detail here.

The functions of the invention can thus be implemented in the mobile station preferably by software. Software comprising the necessary functional commands can be located in connection with the control unit 316. The softwa-
30 re may naturally have a modular structure, i.e. it may comprise several separate programs that can be updated separately from, for example, the computer system or the radio network operator.

The solution of the invention can also be applied to mobile stations which are equipped with more than one SIM/USIM card. Such mobile stations
35 include, for example, telephones that enable "pre-paid" SIM/USIM cards to be used. Such a mobile station enables a solution wherein only one card is used

for establishing a connection. In an embodiment of the invention, some of the information necessary for encryption is obtained from the card which is not used in establishing the connection.

Examine next another preferred embodiment of the invention. When
 5 a connection is being established in the GSM and GPRS systems, for example, both the terminal and the network know an "SRES" (Signed RESult) field. The field is also called an XRES. The field is typically 32 to 128 bits long. In connection with connection setup, the SRES is specified by both parties to the connection by utilizing the particular common parameters and the same
 10 algorithm. In a prior art solution, the SRES is transmitted from the terminal to the network wherein the computed number is compared with the number computed in the network. Further information on the SRES field can be found in M. Mouly, M. P. Pautet: *The GSM System for Mobile Communications*. ISBN 2-9507190-0-7, chapter 7.2.2.1, for example, which is incorporated herein by
 15 reference.

In the present embodiment of the invention, instead of the SRES only, the terminal transmits information that may comprise fields:

	SRES	signed result,
	TIME	time information,
20	IMSI	international number of the terminal, and
	IMEI	device number of the terminal.

Compared with the prior art, an advantage of this embodiment is, naturally, enhanced protection since it is both time- and device-specific. In GSM-based systems, the international number IMSI of the terminal comprises a national
 25 code, operator code and actual telephone number of the terminal.

Examine next another preferred embodiment of the invention. When the RADIUS protocol is used in connection with the PPP/CHAP method, the authentication server receives fields "chap challenge", "user name" and "chap response" from the terminal. The authentication server compares the "chap
 30 response" generated by itself with the one received from the terminal. In a solution of the present embodiment of the invention, the fields have values:

	"chap challenge"	SRES,
	"user name"	user name to the system, and
	"chap response"	word formed from the values
35		IMSI, IMEI, PIN, time,
		SRES.

Since the fields include the user name in plain text, the authentication server is thus able to quickly select from its own database the other information and generate a time-dependent, local "chap response", which thus has to correspond with the one received from the terminal.

5 Furthermore, in another preferred embodiment of the invention, a modified PPP/PAP method is utilized in connection with the RADIUS protocol. In the PPP/PAP method, the user name and password were originally transmitted unencrypted over the transmission path, in which case protection was weak. In the solution of the invention, an encrypted identifier based on the
10 values IMSI, IMEI, PIN, time, SRES and generated according to the invention is thus transmitted in the field reserved for the user name. The SRES is transmitted in the field reserved for the password. Further, the user name to the system is transmitted in the "calling station id" field. This is to enable the authentication server to identify the caller without going through all potential
15 users. When the RADIUS method is used, the field reserved for the password (in which the SRES is now transmitted) can be protected by using the common key of the GGSN and a company network. In a solution of the present embodiment of the invention, the fields thus have values:

20	"user name"	word formed from the values IMSI, IMEI, PIN, time, SRES,
	"user password"	SRES, and
	"calling station id"	user name to the system.

25 In a preferred embodiment of the invention, in the alternatives described above the user name to the system is the same as the user's telephone number in the ISDN form, i.e. a number called an MSISDN. Further information on this can be found in M. Mouly, M. P. Pautet: *The GSM System for Mobile Communications*. ISBN 2-9507190-0-7, chapter 8.1.1., for example, which is incorporated herein by reference.

30 Although the invention has been described above with reference to the example according to the accompanying drawings, it is obvious that the invention is not restricted thereto but can be modified in many ways within the scope of the inventive idea disclosed in the attached claims.

0969874-30290

CLAIMS

1. A method of reliably identifying a user in a computer system, in which method a mobile station is used for communicating with the computer system and a personal identification number is supplied into the mobile station, the method comprising the steps of:
 - generating a first one-time password in the mobile station without any action by the user by utilizing a known algorithm on the basis of a personal identification number of the user, subscriber-specific identifier read from a subscriber-specific identification module of the mobile station, device-specific identifier of the mobile station and time,
 - encoding the first one-time password and the subscriber-specific identifier of the user at the mobile station,
 - transmitting the encoded password and subscriber-specific identifier to an authentication server of the computer system,
 - identifying the user at the authentication server on the basis of the subscriber-specific identifier, and
 - searching a database for the personal identifier number of the user and the device-specific identifier of the mobile station associated with the user,
 - generating a second one-time password at the authentication server by utilizing the predetermined algorithm on the basis of the personal identification number of the user, subscriber-specific identifier, device-specific identifier of the mobile station and time,
 - comparing the first password and the second password with each other at the authentication server, and if the passwords match,
 - enabling the telecommunication connection between the mobile station of the user and the computer system.
2. A method as claimed in claim 1, wherein the mobile station synchronizes the timing of the mobile station with the timing of the authentication server before the identification procedure is started.
3. A method as claimed in claim 1, wherein the user is identified automatically when the user starts an application utilizing the computer system in the mobile station.
4. A method as claimed in claim 1, wherein the authentication server transmits no information to the mobile station if the first and the second passwords do not match.

5. A method as claimed in claim 1, wherein during the identification, the terminal transmits to the authentication server a message comprising at least a field comprising a SRES value, a field comprising time, a field comprising an international telephone number of the terminal, and a field comprising a device number of the terminal.

6. A method as claimed in claim 1, wherein during the identification, a PPP/CHAP protocol is used in connection with a RADIUS protocol, and the terminal transmits to the authentication server a message comprising at least a field comprising a SRES value, a field comprising a user name to the system, and a field comprising a password generated from a device identifier, subscriber-specific identifier of the user, personal identification number of the user, time and the SRES value.

7. A method as claimed in claim 1, wherein during the identification, a PPP/PAP protocol is used in connection with the RADIUS protocol, and the terminal transmits to the authentication server a message comprising at least a field comprising a password generated from the device identifier, subscriber-specific identifier of the user, personal identification number of the user, time, and SRES value, a field comprising a SRES value, and a field comprising a user number to the system.

8. A method as claimed in any one of preceding claims 1 to 7, wherein information necessary for encryption is stored in the terminal in more than one subscriber-specific identification module.

9. A method as claimed in claim 6 or 7, wherein the user name to the system is the user's MSISDN.

10. An arrangement for reliably identifying a user in a computer system, which arrangement comprises

a mobile station used for communicating with the computer system, the mobile station comprising

a subscriber-specific identification module comprising a subscriber-specific identifier,

a device-specific identifier permanently encoded in the mobile station,

means for reading a personal identifier number which is supplied by the user and which enables the device to be used,

means for checking the correctness of the identifier number always before the device is put to use, and

0022014285960

which arrangement comprises an authentication server comprising memory means for storing the user names of the users in the system and the corresponding personal identifiers and device-specific identifiers, the mobile station further comprising

5 means for generating a first one-time password without any action by the user by utilizing a known algorithm on the basis of the personal identification number of the user, subscriber-specific identifier read from a subscriber-specific identification module of the mobile station, device-specific identifier of the mobile station and time,

10 means for encoding the first one-time password and the subscriber-specific identifier of the user,

means for transmitting the encoded password and subscriber-specific identifier to an authentication server of the computer system, and the authentication server is further arranged to

15 identify the user on the basis of the subscriber-specific identifier, and search a database for the personal identifier number of the user and the device-specific identifier of the mobile station associated with the user,

generate a second one-time password at the authentication server by utilizing the predetermined algorithm on the basis of the personal identification number of the user, subscriber-specific identifier, device-specific identifier of the mobile station and time,

20 compare the first password and the second password with each other at the authentication server, and if the passwords match, enable the telecommunication connection between the mobile station of the user and the computer system.

11. An arrangement as claimed in claim 10, wherein the mobile station is arranged to synchronize the timing of the mobile station with the timing of the authentication server before the identification procedure is started.

30 12. An arrangement as claimed in claim 10, wherein the mobile station is arranged to identify the user automatically when the user starts an application utilizing the computer system in the mobile station.

13. An arrangement as claimed in claim 10, wherein the authentication server is arranged not to transmit any information to the mobile station if the first and the second passwords do not match.

35 14. An arrangement as claimed in claim 10, wherein the mobile station is arranged to transmit to the authentication server a message comprising

at least a field comprising a SRES value, a field comprising time, a field comprising an international telephone number of the terminal, and a field comprising a device number of the terminal.

- 5 15. An arrangement as claimed in claim 10, wherein the mobile station and the authentication server are arranged to use a PPP/CHAP protocol in connection with a RADIUS protocol during the identification, and the terminal is arranged to transmit to the authentication server a message comprising at least a field comprising a SRES value, a field comprising a user name to the system, and a field comprising a password generated from a device identifier, subscriber-specific identifier of the user, personal identification number of the user, time and the SRES value.

- 15 16. An arrangement as claimed in claim 10, wherein the mobile station and the authentication server are arranged to use a PPP/PAP protocol in connection with the RADIUS protocol during the identification, and the mobile station is arranged to transmit to the authentication server a message comprising at least a field comprising a password generated from the device identifier, subscriber-specific identifier of the user, personal identification number of the user, time, and SRES value, a field comprising a SRES value, and a field comprising a user number to the system.

- 20 17. An arrangement as claimed in claims 15 or 16, wherein the user name to the system is the user's MSISDN.

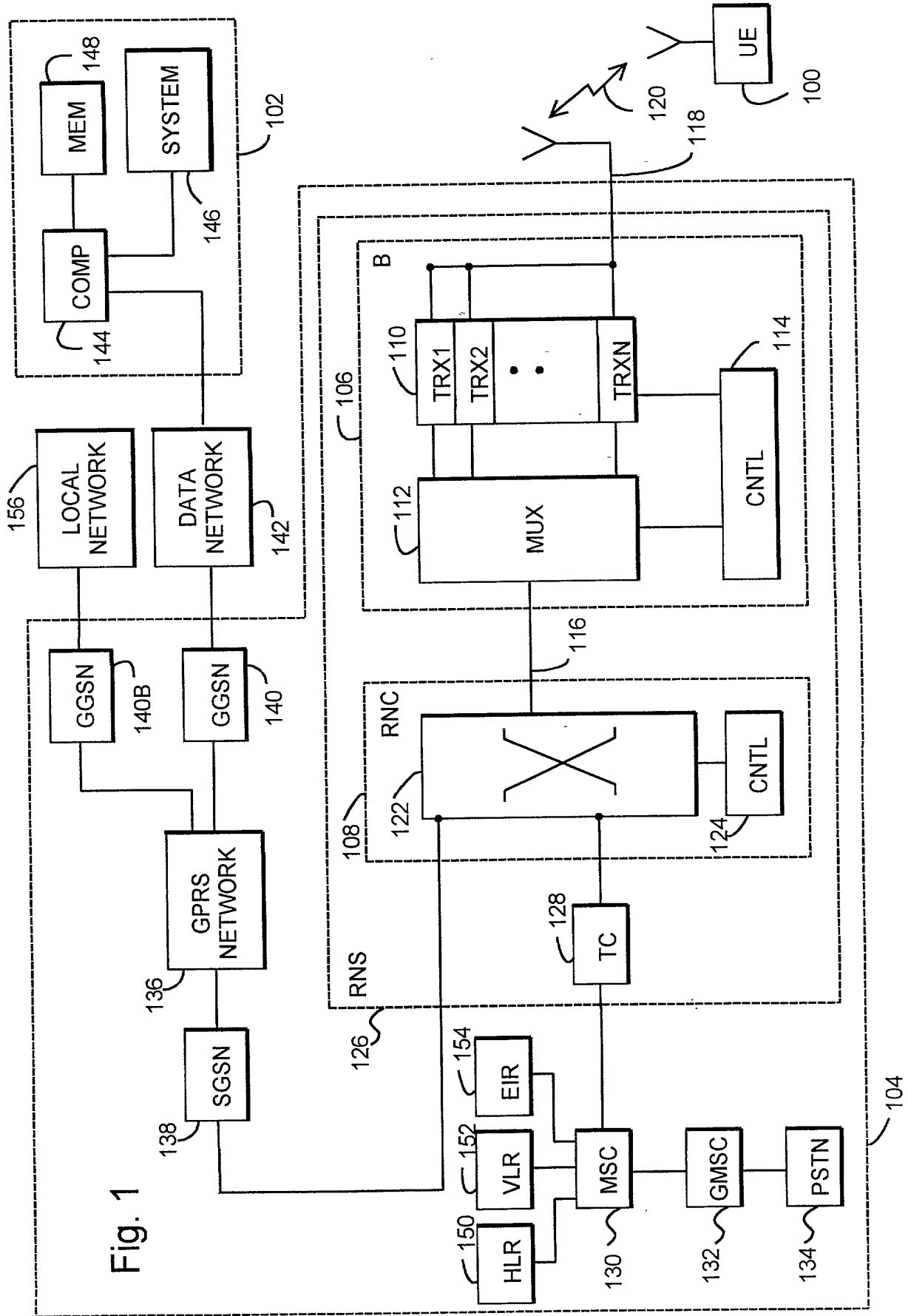
 18. An arrangement as claimed in any one of preceding claims 10 to 17, wherein the mobile station is a GPRS system mobile station.

- 25 19. An arrangement as claimed in any one of preceding claims 10 to 17, wherein the mobile station comprises more than one subscriber-specific identification module, and information necessary for encryption is stored in more than one identification module.

ABSTRACT

The invention relates to an arrangement and a method for reliably identifying a user in a computer system. The method utilizes a mobile station for communicating with the system. The method comprises generating a first one-time password in the mobile station by utilizing a known algorithm on the basis of the identification number of the user, subscriber-specific identifier, device-specific identifier of the mobile station, and time. The password obtained and the subscriber-specific identifier of the user are encoded and transmitted to an authentication server of the computer system, comprising identifying the user on the basis of the subscriber-specific identifier, searching a database for the personal identifier number of the user and the device-specific identifier of the mobile station associated with the user, generating a second password at the authentication server by utilizing the same predetermined algorithm on the basis of the personal identification number of the user, subscriber-specific identifier, device-specific identifier of the mobile station and time, comparing the first and the second passwords with each other at the authentication server, and if the passwords match, enabling the telecommunication connection between the mobile station and the computer system.

(Figure 1)



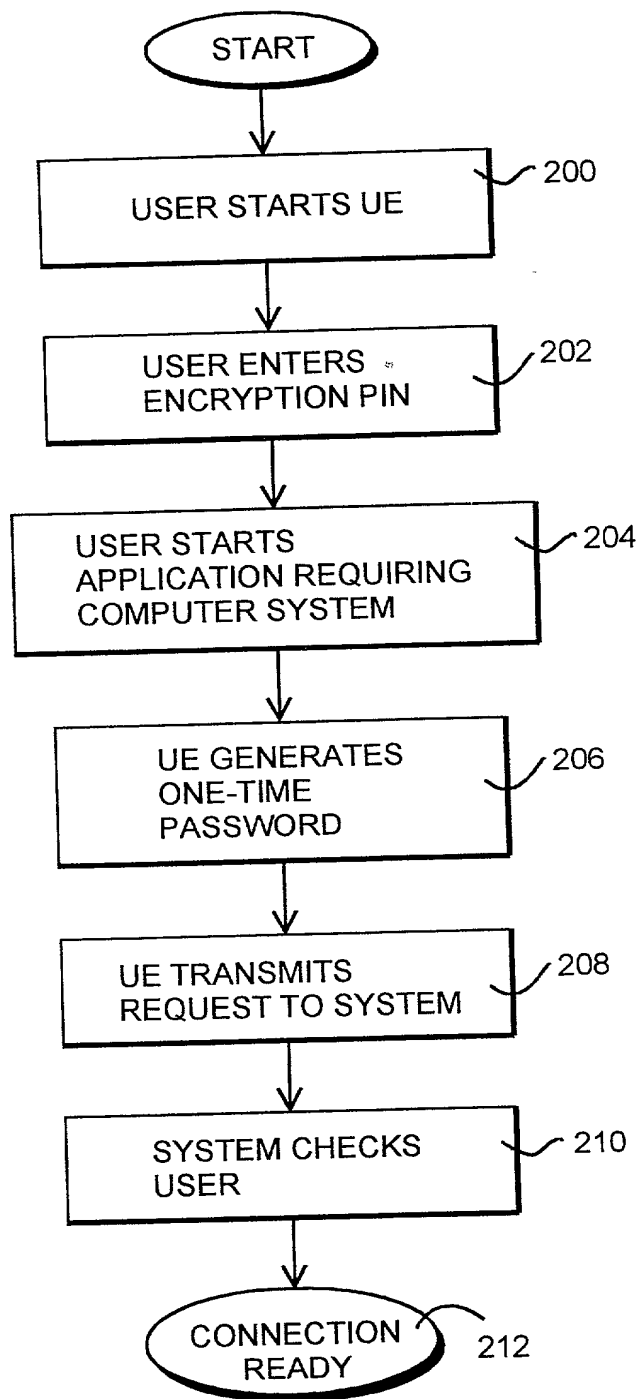


Fig. 2a

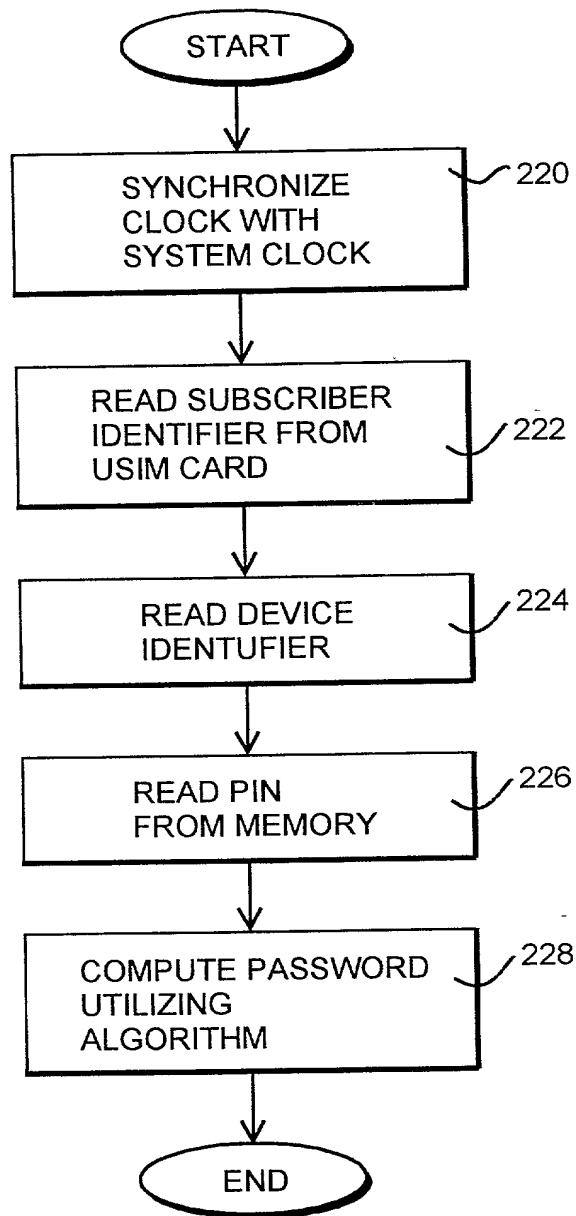


Fig. 2b

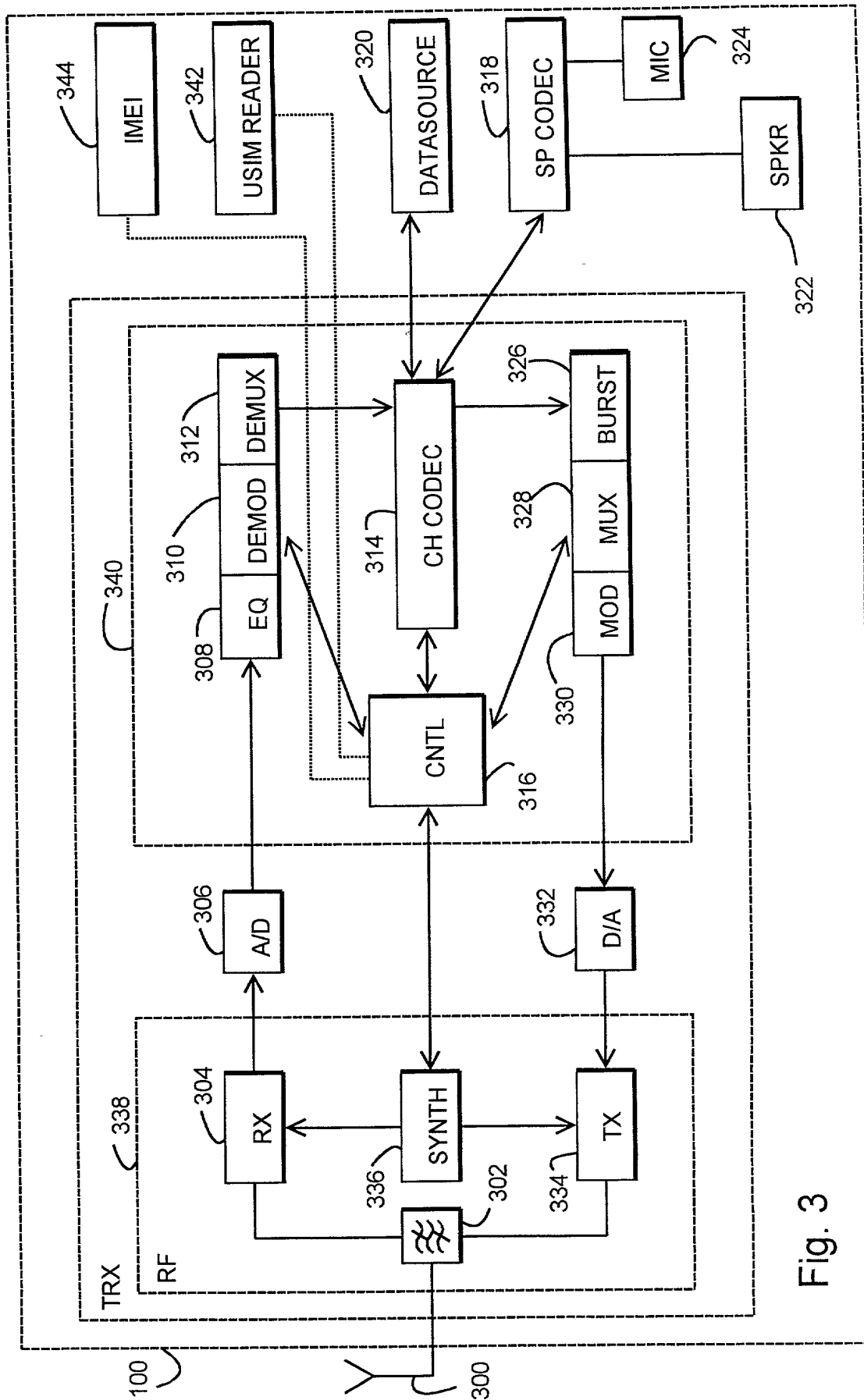


Fig. 3